01-09-06

AF/3621

PTO/SB/21 (09-04)

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/825,971
Filing Date	April 16, 2004
First Named Inventor	VanFleet, Steven L.
Art Unit	3621
Examiner Name	Evens J. Augustin
Attorney Docket Number	020375-050000US

Total Number of Pages in This Submission

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):
  Return Postcard

Remarks: The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Townsend and Townsend and Crew LLP		
Signature	Patrick M. Boucher		
Printed name	Patrick M. Boucher		
Date	January 5, 2006	Reg. No.	44,037

CERTIFICATE OF TRANSMISSION/MAILING

Express Mail Label: EV 780617805 US

I hereby certify that this correspondence is being deposited with the United States Postal Service with "Express Mail Post Office to Address" service under 37 CFR 1.10 on this date January 5, 2006 and is addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	Nina L. McNeill		
Typed or printed name	Nina L. McNeill	Date	January 5, 2006

"Express Mail" Label No. EV780617805US
Date of Deposit January 5, 2006

PATENT
Attorney Docket No.: 020375-050000US

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to Address" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By: Nina L. McNeill
Nina L. McNeill

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:	Examiner: Augustin, Evens J.
Steven L. VanFleet	Art Unit: 3621
Application No.: 10/825,971	APPEAL BRIEF UNDER 37 CFR §41.37
Filed: April 16, 2004	
For: METHODS AND SYSTEMS FOR ONLINE TRANSACTION PROCESSING	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellant offers this Brief further to the Notice of Appeal mailed on October 12, 2005.

1. Real Party in Interest

The real party in interest is First Data Corporation.

2. Related Appeals and Interferences

No prior or pending appeals, interferences, or judicial proceedings are known that are related to, will directly affect, will be directly affected by, or have a bearing on the Board decision in this appeal.

3. Status of Claims

Claims 1 – 25 are pending in the application. All of these claims stand rejected pursuant to a Final Office Action mailed May 24, 2005 ("the Final Office Action").

The rejections of each of Claims 1 – 25 are believed to be improper and are the subject of this appeal. Under the Office's pilot pre-appeal-brief review program, a pre-appeal-brief conference was held and a decision mailed December 6, 2005 to proceed to the Board.

4. Status of Amendments

No amendments have been filed subsequent to the mailing of the Final Office Action on May 24, 2005.

5. Summary of Claimed Subject Matter

The claimed invention relates to online transaction processing, particularly to methods and systems that permit debit transactions to be performed as part of online transaction processing (Application, p. 1, ll. 17 – 19). It is well known that the prevalence of transactions over the Internet has been increasing over the last several years, permitting consumers to use such online transactions for the purchase of a variety of goods and/or services (*id.*, p. 1, ll. 21 – 23). By far, such transactions have been dominated by credit models in which a consumer provides a credit-card number to an online merchant, who obtains authorization for the credit

transaction in much the same manner as is done in traditional brick-and-mortar transactions (*id.*, p. 29 – 31).

The prevalence of credit-based transactions in the online environment is a reflection of the barriers that exist to implementing debit-based transactions (*id.*, p. 2, ll. 12 – 15). A debit transaction differs from a credit transaction in that funds are accessed from a financial institution during execution of a transaction (*id.*, p. 2, ll. 24 – 25). From the perspective of merchants, such a capability has the attractive feature that it permits the transactions to be guaranteed to the merchants by allocating specific funds identified in a financial account to the transaction (*id.*, p. 2, ll. 10 – 12). This is in contrast to the dominant credit transactions, which are not guaranteed to merchants and expose the merchant to the risk of certain types of fraud (*id.*, p. 2, ll. 4 – 9).

a. Independent Claim 1

The invention as claimed provides an effective mechanism for implementing debit transactions in an online environment. Independent Claim 1 recites a method for coordinating an Internet-based financial transaction between an Internet merchant and a customer. A first information packet is received with a payment network (*id.*, Fig. 1, element 100) from the Internet merchant (*id.*, Fig. 1, element 108). The first information packet comprises a credential assigned to the customer (*id.*, Fig. 1, element 104) and transaction information that specifies at least a cost of the transaction (*id.*, p. 11, ll. 9 – 14). The payment network uses the credential to determine account information and authorization information (*id.*, p. 11, ll. 14 – 19) — the account information identifies a financial account maintained by the customer at a financial institution and the authorization information allows debit access to the identified financial account (*id.*, p. 11, ll. 16 – 17). *See* block 428 of Fig. 4B; the "first information packet" recited in the claim corresponds to the "authentication packet" in some embodiments.

The payment network generates a second information packet that comprises the transaction information, the account information, and the authorization information (*id.*, p. 11, ll. 19 – 21). *See also* block 434 of Fig. 4B; the "second information packet" recited in the claim

corresponds to the "authorization packet" in some embodiments. The second information packet is transmitted with the payment network to the financial institution with a request to perform a debit transaction in support of the transaction (*id.*, p. 12, ll. 17 – 19; *see also id.*, Fig. 4B, element 434).

b. Independent Claim 10

Independent Claim 10 is generally different in scope that Claim 1. In some respects, it is narrower, reciting additional specific details of a method for coordinating an Internet-based financial transaction between an Internet merchant and a customer and including guarantee and loyalty-program functionality. In other respects, it is broader — similarly to independent Claim 1, a first information packet is received with a payment network (*id.*, Fig. 1, element 108), but there is no requirement that the first information packet be received from the Internet merchant. In this instance, the first information packet comprises an electronic file having encrypted content and transaction information that specifies at least a cost of the transaction (*id.*, p. 11, ll. 9 – 14; p. 10, ll. 6 – 8). The electronic file is decrypted with the payment network to recover a primary account number ("PAN") and personal identification number ("PIN") that respectively act as account information and authorization information that allows debit access to the account (*id.*, p. 11, ll. 14 – 17; p. 10, ll. 8 – 11).

A second information packet is generated with the payment network to comprise the transaction information, the PAN, and the PIN (*id.*, p. 11, ll. 17 – 21) and is transmitted with the payment network to the financial institution with a request to perform a debit transaction (*id.*, p. 12, ll. 16 – 19). A response is received from the financial institution indicating approval or denial of the debit transaction (*id.*, p. 12, ll. 1 – 4; *see also id.*, Fig. 4B, block 446). The payment network determines whether to provide a guarantee of the transaction to the merchant (*id.*, Fig. 4B, block 438; *id.*, p. 12, ll. 3 – 10). The specification provides examples of how such a determination may be made, such as by performing a risk analysis that accounts for such factors as transaction size, credit history, etc. (*id.*, p. 12, ll. 4 – 8). A determination is also made whether to credit a loyalty program for the customer (*id.*, Fig. 4B, block 448; p. 13, ll. 8 – 16), illustrating

an integration of the method for executing the debit transaction with loyalty functionality. The authorization code indicating approval or denial of the transaction is transmitted, such as back to the merchant directly or through an intermediary (*id.*, Fig. 4B, blocks 450 and 452; *id.*, p. 13, ll. 19 – 20).

c. Independent Claim 14

Independent Claim 14 is an apparatus claim that recites elements of the payment network (*id.*, Fig. 1, element 100) itself. The payment network comprises a communications device (*id.*, Fig. 3, element 314; *id.*, p. 8, l. 11), a processor (*id.*, Fig. 3, element 302; *id.*, p. 8, l. 9), a storage device (*id.*, Fig. 3, element 308; *id.*, p. 8, l. 10), and a memory (*id.*, Fig. 3, element 318; *id.*, p. 8, l. 12). The memory is coupled with the processor and comprises a computer-readable medium having a computer-readable program to direct operation of the payment network (*id.*, Fig. 3, elements 320, 322, and 324; *id.*, p. 8, ll. 22 – 28). The computer-readable program includes instructions specifically recited in the claim to implement the method of independent Claim 1. Details of the method are accordingly not repeated here.

6. Grounds of Rejection to be Reviewed on Appeal

1. Whether Claims 1 – 7, 9, 14 – 23, and 25 are anticipated under 35 U.S.C. §102(e) by U.S. Pat. No. 6,609,113 ("O'Leary"). Section 3 of the Final Office Action describes the Examiner's position on this issue, supplemented by certain remarks in Section 1, captioned "Response to Arguments."

2. Whether Claims 8, 10 – 13, and 24 are unpatentable under 35 U.S.C. §103(a) over O'Leary in view of U.S. Pat. Publ. No. 2001/0054003 ("Chien"). Section 5 of the Final Office Action describes the Examiner's position on this issue, supplemented by certain remarks in Section 1, captioned "Response to Arguments."

7. Argument

1. Whether Claims 1 – 7, 9, 14 – 23, and 25 are anticipated by O'Leary

For a rejection to be maintained under §102, the Examiner is charged with establishing that every limitation recited in the claims is taught in the cited reference, either expressly or inherently. Manual of Patent Examining Procedure, Eighth Edition, Second Revision, August 2005 (hereinafter "MPEP") 2131. At least certain limitations of independent Claim 1 and corresponding limitations of independent Claim 14 are not taught or suggested by O'Leary.

O'Leary is directed generally to retail transactions conducted over the Internet (O'Leary, Col. 1, ll. 15 – 20; Col. 1, l. 22 – 27), and Applicants accordingly have no quarrel with its general relevance to the application. But how O'Leary teaches implementing techniques for processing Internet payments is distinct from what is claimed. In particular, O'Leary makes a distinction between traditional "pull" models of making payment, in which a "seller 'pulls' the payment from the buyer's account using a debit instruction" (O'Leary, Col. 8, ll. 55 – 56), and "push" models of its invention, in which a "buyer 'pushes' a credit to the seller's account" (*id.*, Col. 8, ll. 57 – 58). The claims in the Application are directed to an improved arrangement that uses what O'Leary characterizes as a "pull" model and is unlike the specific "push" model that O'Leary itself teaches as a "new paradigm" for conducting Internet transactions (*id.*, Col. 4, l. 38).

The "push" model taught by O'Leary is implemented with a structure like that illustrated in Fig. 2 of O'Leary and makes use of a number of different components that include a "payment portal processor" ("PPP") 227, a digital Wallet 215, an Internet Pay Anyone ("IPA") Account 230, and a Virtual Private Lockbox ("VPL") 235 (*id.*, Col. 4, ll. 54 – 65). These components act in concert with an Electronic Funds Transfer ("EFT") network to enable credits to be pushed from a user's IPA Account 230 to other accounts over the EFT network (*id.*, Col. 4, ll. 60 – 65).

As taught by O'Leary, when a user wishes to purchase goods and/or services from an Internet merchant, the user finds the merchant's web site 255 and completes a certification

process by keying in a userid and password (*id.*, Col. 15, ll. 33 – 65). O'Leary teaches that these steps may be performed in either order, and that the user may find the merchant web site himself or may be directed to it by the system (*id.*, Col. 15, ll. 46 – 51; Col. 15, ll. 60 – 62). In any event, completing the certification procedure acts to identify the user to the PPP and thereby identify the user's account information. The system is activated to coordinate the transaction once the user has selected an item for purchase and activated the digital Wallet 215. In response, the merchant web site "generates and transmits to the user a bill payment message containing information with respect to the prospective purchase" (*id.*, Col. 15, l. 66 – Col. 16, l. 1). This bill payment message includes information identifying the *merchant* account (such as with a merchant BIN and account number), a transaction identifier, and the cost of the transaction (*id.*, Col. 16, ll. 1 – 5). User funds to support the transaction are provided from the IPA Account 230 (which may be replenished from a user demand deposit account if necessary, *see id.*, Col. 16, ll. 22 – 28). Upon approval from the user, a payment authorization message 225 is generated that includes the merchant payee information (*id.*, Col. 16, ll. 28 – 35).

The payment authorization message 225 is transmitted to the user's bank 220, which debits the IPA account 230 to generate "an EFT credit message in the amount of the authorized payment" (*id.*, Col. 17, ll. 11 – 14). This credit message is transferred to the merchant VPL and acts as a guarantee of payment from the user's bank to the merchant's bank to effect payment (*id.*, Col. 17, ll. 23 – 30). Various settlement and reconciliation procedures may subsequently be performed to effect multiple payments made in this way among various merchants and users (*id.*, Col. 17, ll. 27 –58).

What is notable about this arrangement is the fact that the user's account information is never made available to the merchant. This fact is a specific point of emphasis in O'Leary:

> The present invention completely solves one of the biggest problems of the prior art, the hesitancy of a consumer to provided financial account information over the Internet. Rather than the merchant "pulling" in the consumer[']s account information and requiring authentication of the consumer, the PPP enhanced Wallet 215 "pushes" an EFT credit message to the merchant's Virtual Private Lockbox, without the merchant ever obtaining the consumer[']s account information.
> (*Id.*, Col. 18, ll. 23 – 31, emphasis added)

Thus, in comparing what O'Leary discloses with what is recited in independent Claims 1 and 14, it is readily apparent that O'Leary fails to teach or suggest the combination of limitations of "receiving ... a first information packet from the Internet merchant [that] compris[es] a credential assigned to the customer" and of "determining from the credential ... account information that identifies a financial account maintained by the customer" (emphases added). Indeed, the very purpose of the arrangement described in O'Leary is to prevent the Internet merchant from ever having access to information that permits determination of the customer's account information.

The Final Office Action attempts to draw a correspondence between O'Leary's description of a "transaction ID" with the "credential" recited in the claims:

> In particular O'Leary et al. teaches that the merchant assigns the buyer a unique transaction ID (credential), which has to be reconciled/validated during an Electronic Fund Transfer (EFT) (column 14, lines 58 -63). The merchant transmits to the system the transaction ID/credential, along with the dollar amount of the transaction (cost of transaction) (column 16, lines 1-5). (Final Office Action, p. 2, ll. 10 – 14).

Such a correspondence is misplaced. Although the transaction ID is received from the merchant in O'Leary, its stated purpose is to allow "the recipient of the credit ... to match the received credit with a proposed purchase" (O'Leary, Col. 14, ll. 47 – 58). Rather than determine account information from the "transaction ID," access to the user's account is instead made through the Wallet functionality, identified by the certification information received from the user, such as described at Col. 16, ll. 18 – 45 of O'Leary. While not directly relevant to a §102 analysis, it is notable that O'Leary itself pointedly emphasizes that "the EFT credit message is completely different from traditional EFT messages that are debits" (O'Leary, Col. 17, ll. 14 – 16) in distinguishing its "push" methodology from a "pull" technique like that claimed.

Since a limitation recited in each of independent Claims 1 and 14 is not taught or suggested by O'Leary, those claims are believed to be patentable over O'Leary, as are each of Claims 2 – 7, 9, 15 – 23, and 25, which depend from either of Claim 1 and 14.

2. Whether Claims 8, 10 – 13, and 24 are unpatentable over O'Leary in view of Chien

For a rejection to be maintained under §103(a), the Examiner is charged with factually supporting a *prima facie* case of obviousness. MPEP 2142. Such a *prima facie* case requires, *inter alia*, that all limitations of the claims be taught or suggested by the cited references and that there be some suggestion or motivation to combine and/or modify the reference teachings as the Examiner proposes. MPEP 2143.

Claims 8 and 24 depend respectively from Claims 1 and 14 and are believed patentable by virtue of that dependency and the patentability of Claims 1 and 14 as explained above.

With respect to Claims 10 – 13, it was noted above that certain of the language in independent Claim 10 is narrower than in independent Claim 1, reciting additional steps and further limiting the information retrieved from the first information packet. Applicants acknowledge that Claim 10 is, at the same time, broader than Claim 1 by not requiring that the first information packet be received from the Internet merchant. But Claim 10 still requires receipt by the payment network of a first information packet that comprises both "an electronic file having encrypted content," which when decrypted "identifies a financial account maintained by the customer," and "transaction information." O'Leary teaches separate receipt of these two components, one from the user and one from the Internet merchant, and fails to teach receipt of "a first information packet" that includes both. This deficiency is not remedied by the additional citation of Chien, which is relied on only for its disclosure of loyalty functions.

The Final Office Action responds to this observation by citing *In re Larson*, 340 F.2d 965, 144 USPQ 347 (CCPA 1965) for the proposition that "making integral what had been made previously [is] not patentable." The position expressed is that receipt of a first information packet that includes everything recited in the claim amounts to "making integral" what is taught in O'Leary.

It is respectfully believed that the Final Office Action overstates the holding of *Larson*. The claim under consideration in *Larson* was directed to a mechanical device and recited "a brake drum integral with a said clamping means." *Larson*, 340 F.2d at 968, 144 USPQ at 349. The prior art taught a brake disc "rigidly secured" to a clamping means. *Id.*, 340 F.2d at 968, 144 USPQ at 349. The principal focus of *Larson* was the interpretation of "integral," with the CCPA agreeing with the Board's construction of the term as "not limited to a fabrication of the parts from a single piece of metal, but ... inclusive of other means for maintaining the parts fixed together as a single unit." *Id.*, 340 F.2d at 968, 144 USPQ at 349. Within this context, i.e. with an acknowledgment that the claim term was "inclusive of other means for maintaining the parts fixed together as a single unit," the CCPA also agreed with the Board that use of a one-piece construction instead of the "rigidly secured" structure of the prior art was a matter of obvious engineering choice. *Id.*, 340 F.2d at 968, 144 USPQ at 349.

What *Larson* holds is that the term "integral" in a claim to a mechanical device is broader than requiring parts be fabricated from a single piece, and does not distinguish over prior art that teaches rigidly securing the parts. Such a holding is distinct from the current issue in a number of respects. First, the term "integral" does not appear in the claim so its interpretation is irrelevant. In addition, Claim 10 is a not directed to a mechanical structure so the analogy with *Larson* is at best indirect — but even attempting the analogy, the prior art does not disclose any analogy to "rigidly securing" the components of the "first information packet." Indeed, it is a central preoccupation of O'Leary to ensure that the merchant never has access to the user's financial account information (*see, e.g.*, O'Leary, Col. 18, ll. 20 – 35). Part of effecting this goal is to keep the customer financial account information separate from the transaction information. Thus, completely unlike the situation in *Larson*, in which the prior art taught "rigidly securing" parts that were attempted to be distinguished from those that were "integral," the prior art here specifically teaches reasons for maintaining the separateness of the components of the "first information packet." The Final Office Action identifies no motivation to modify O'Leary to combine those components. Instead, it is clear that O'Leary's emphasis on preventing access by the merchant to the user's financial account information very much teaches away from what is

claimed. To modify O'Leary as proposed would render it unsatisfactory for one of its intended purposes, a factor that evidences the *non*obviousness of the modification. MPEP 2143.01.V.

For these reasons, Claim 10 is respectfully believed to be patentable, as are each of Claims 11 – 13 by virtue of their dependence from Claim 10.

8. Conclusion

Appellant believes that the above discussion is fully responsive to all grounds of rejection set forth in the application. Please deduct the requisite fee of $500.00 pursuant to 37 C.F.R. §1.17(c) from Deposit Account 20-1430 and any additional fees that may be due in association with the filing of this Brief.

Respectfully submitted,

Patrick M. Boucher
Reg. No. 44,037

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
PMB:pmb
60669849 v1

CLAIMS APPENDIX

The claims involved in this appeal are as follows:

1. (Original) A method for coordinating an Internet-based financial transaction between an Internet merchant and a customer, the method comprising:

receiving, with a payment network, a first information packet from the Internet merchant, the first information packet comprising a credential assigned to the customer and transaction information specifying at least a cost of the Internet-based financial transaction;

determining from the credential, with the payment network, account information that identifies a financial account maintained by the customer at a financial institution and authorization information that allows debit access to the identified financial account;

generating, with the payment network, a second information packet comprising the transaction information, the account information, and the authorization information; and

transmitting, with the payment network, the second information packet to the financial institution with a request to perform a debit transaction from the identified financial account for the specified cost of the Internet-based financial transaction.

2. (Original) The method recited in claim 1 further comprising:

receiving, with the payment network, a response from the financial institution indicating approval or denial of the debit transaction; and

transmitting, with the payment network, an authorization code to the Internet merchant indicating approval or denial of the Internet-based financial transaction in accordance with the response received from the financial institution.

3. (Original) The method recited in claim 2 further comprising:

performing, with the payment network, a risk analysis of the Internet-based financial transaction; and

determining, with the payment network, whether to provide a guarantee of the Internet-based transaction to the Internet merchant based on the risk analysis,

wherein the authorization code further reflects whether the guarantee is provided.

4. (Original) The method recited in claim 1 wherein the second information packet is transmitted to the financial institution over an automated clearing house ("ACH") network.

5. (Original) The method recited in claim 1 wherein the second information packet is transmitted to the financial institution over a debit system.

6. (Original) The method recited in claim 1 wherein the second information packet is transmitted directly to the financial institution from the payment network.

7. (Original) The method recited in claim 1 wherein:

the account information comprises a primary account number ("PAN") for the identified financial account; and

the authorization information comprises a personal identification number ("PIN") assigned to the customer for accessing the identified financial account.

8. (Original) The method recited in claim 1 further comprising crediting, with the payment network, a loyalty program for the customer in response to execution of the Internet-based financial transaction.

9. (Original) The method recited in claim 1 wherein:

the credential comprises an electronic file having encrypted content received from the customer; and

determining account information comprises decrypting the encrypted content.

10. (Original) A method for coordinating an Internet-based financial transaction between an Internet merchant and a customer, the method comprising:

receiving, with a payment network, a first information packet comprising an electronic file having encrypted content and transaction information specifying at least a cost of the Internet-based financial transaction;

decrypting the electronic file, with the payment network, to recover a primary account number ("PAN") that identifies a financial account maintained by the customer at a financial institution and to recover a personal identification number ("PIN") assigned to the customer for accessing the identified financial account;

generating, with the payment network, a second information packet comprising the transaction information, the PAN, and the PIN;

transmitting, with the payment network, the second information packet to the financial institution with a request to perform a debit transaction from the identified financial account for the specified cost of the Internet-based financial transaction;

receiving, with the payment network, a response from the financial institution indicating approval or denial of the debit transaction;

determining, with the payment network, whether to provide a guarantee of the Internet-based transaction to the Internet merchant;

determining, with the payment network, whether to credit a loyalty program for the customer; and

transmitting, with the payment network, an authorization code indicating approval or denial of the Internet-based transaction.

11. (Original) The method recited in claim 10 wherein:

the first information packet includes an identification of the Internet merchant; and

determining whether to provide the guarantee of the Internet-based transaction comprises determining whether the Internet merchant is one of an identified list of Internet merchants who request guarantees of all Internet-based financial transactions.

12. (Original) The method recited in claim 10 wherein determining whether to provide the guarantee of the Internet-based transaction comprises determining whether the transaction information is consistent with a predefined set of parameters.

13. (Original) The method recited in claim 10 wherein the first information packet further comprises a request from the Internet merchant for the guarantee of the Internet-based transaction.

14. (Original) A payment network comprising:

a communications device;

a processor;

a storage device; and

a memory coupled with the processor, the memory comprising a computer-readable medium having a computer-readable program embodied therein for directing operation of the payment network, the computer-readable program including:

instructions for receiving, with the communications device, a first information packet from the Internet merchant, the first information packet comprising a credential assigned to the customer and transaction information specifying at least a cost of the Internet-based financial transaction;

instructions for determining from the credential, with the processor, account information that identifies a financial account maintained by the

customer at a financial institution and authorization information that allows debit access to the identified financial account;

instructions for generating, with the processor, a second information packet comprising the transaction information, the account information, and the authorization information; and

instructions for transmitting, with the communications device, the second information packet to the financial institution with a request to perform a debit transaction from the identified financial account for the specified cost of the Internet-based financial transaction.

15. (Original) The payment network recited in claim 14 wherein the computer-readable program further includes:

instructions for receiving, with the communications device, a response from the financial institution indicating approval or denial of the debit transaction; and

instructions for transmitting, with the communications device, an authorization code to the Internet merchant indicating approval or denial of the Internet-based financial transaction in accordance with the response received from the financial institution.

16. (Original) The payment network recited in claim 15 wherein the computer-readable program further includes:

instructions for performing, with the processor, a risk analysis of the Internet-based financial transaction; and

instructions for determining, with the processor, whether to provide a guarantee of the Internet-based transaction to the Internet merchant based on the risk analysis,

wherein the authorization code further reflects whether the guarantee is provided.

17. (Original) The payment network recited in claim 16 wherein:

the first information packet includes an identification of the Internet merchant; and

the instructions for determining whether to provide the guarantee of the Internet-based transaction comprise instructions for determining whether the Internet merchant is one of an identified list stored on the storage device of Internet merchants who request guarantees of all Internet-based financial transactions.

18. (Original) The payment network recited in claim 16 wherein the instructions for determining whether to provide the guarantee of the Internet-based transaction comprise instructions for determining whether the transaction information is consistent with a predefined set of parameters.

19. (Original) The payment network recited in claim 16 wherein the first information packet further comprises a request from the Internet merchant for the guarantee of the Internet-based transaction.

20. (Original) The payment network recited in claim 14 wherein:

the communications system is coupled with an automated clearing house ("ACH") network; and

the instructions for transmitting the second information packet to the financial institution comprise instructions for transmitting the second information packet over the ACH network.

21. (Original) The payment network recited in claim 14 wherein the instructions for transmitting the second information packet to the financial institution comprise instructions for transmitting the second information packet over a debit system.

22. (Original) The payment network recited in claim 14 wherein the instructions for transmitting the second information packet comprise instructions for transmitting the second information packet directly to the financial institution from the communications device.

23. (Original) The payment network recited in claim 14 wherein:

the account information comprises a primary account number ("PAN") for the identified financial account; and

the authorization information comprises a personal identification number ("PIN") assigned to the customer for accessing the identified financial account.

24. (Original) The payment network recited in claim 14 wherein the computer-readable program further comprises instructions for crediting, with the processor, a loyalty program for the customer in response to execution of the Internet-based financial transaction.

25. (Original) The payment network recited in claim 14 wherein:

the credential comprises an electronic file having encrypted content received from the customer; and

the instructions for determining account information comprise instructions for decrypting the encrypted content.

EVIDENCE APPENDIX

Not included.

RELATED PROCEEDINGS APPENDIX

Not included.